

PRIVACY IMPACT ASSESSMENT
Account Management Provisioning System (AMPS)

1. **Department of Defense Component:** Defense Logistics Agency.
2. **Name of Information Technology (IT) System:** Account Management Provisioning System (AMPS).
3. **Budget System Identification Number (SNAP-IT Initiative Number):** BIN # 9990
4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository):** 10110.
5. **IT Investment Unique Identifier (OMB Circular A-11):** N/A
6. **Privacy Act System of Records Notice Identifier:** S500.55, entitled "Information Technology Access and Control Records."
7. **OMB Information Collection Requirement Number and Expiration Date:** N/A.
8. **Authority to collect information:** 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Technology; 18 U.S.C. 1029, Access Device Fraud; E.O. 9397 (SSN); and E.O. 10450, Security Requirements for Government Employees, as amended.
9. **Brief summary or overview of the IT system:** AMPS controls, tracks, and routes for approval and action requests for access to DLA's networks, computer systems, and databases that have their access requests managed by AMPS. Requests for access are made on an electronic version of DD Form 2875, entitled "System Authorization Access Request (SAAR)." The point of contact is Gwen Martin in the External Solutions Branch of J6R, 804-279-5391, e-mail: gwen.martin@dla.mil.
10. **Identifiable Information to be Collected and Nature / Source:** PII collected by AMPS are individual's name, Social Security Number (SSN), and citizenship.
11. **Method of information collection:** Information is collected electronically on a secure web site.
12. **Purpose of the collection:** To validate a user's request for access into a DLA system, database, or network that has its access requests managed by AMPS.
13. **Data uses:** The data is used to create an individual's access account within a DLA system, database, or network that has its account access requests managed by AMPS.
14. **Does system derive / create new data about individuals through aggregation?** No.

15. Internal and External Sharing:

Internal to DLA: Data may be shared internally as stated in the Privacy notice. All DLA personnel are required to take Information Assurance (IA) training annually and thus are made aware of the consequences of inappropriately using information contained therein.

External to DLA: Data may also be provided under any of the routine uses published in the system of records notice and/or the DOD "Blanket Routine Uses" published at <http://www.defenselink.mil/privacy/notices/blanket-uses.html>.

16. Opportunities to object to the collection or to consent to the specific uses and how consent is granted:

The form that collects the data contains a Privacy Act Statement as required by 5 U.S.C. 552a (e) (3), allowing the individual to make an informed decision about providing the data. The statement advises that participation is voluntary, and that failure to provide all of the requested data may impede, delay, or prevent further processing of their request.

17. Information provided the individual at Collection, the Format, and the Means of delivery:

A Privacy Act system notice was published in the Federal Register with a 30-day public comment period. Forms that collect personal data contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the DLA HQ Privacy Act Office during the comment period, during data collection, or at any time. If no objections are received, consent is presumed.

18. Data Controls:

Administrative: All requests for access to AMPS roles require appropriate IT clearance levels, approval by the requestor's supervisor, the site security officer, the information owner, and the IA officer. The employee's supervisor must certify within the system that the employee has a valid need for the requested access in order to do their job and that they are the employee's supervisor, the security officer certifies that the clearance levels of the employee requesting the role is equal to or greater than the required clearance on the role, the information owner validates that there are no conflicts with providing the employee access to the requested information and the IA officer validates that all of the required information is provided, all of the required approvals have been obtained and that the employee has completed the mandatory IA training. The SSN is blanked out on the input screen so it is not readable while it is being entered and is only viewable to the security officer during the security review process. All users receive IA training at least yearly and are warned through logon procedures of the conditions associated with access and the consequences of improper activities. All internal DLA users access the system through the use of Common Access Cards (CAC) and are trained to remove their CAC when leaving their desk. DLA computers automatically lock upon removal of the CAC or after a preset period of inactivity with reentry controlled by reentering the CAC Personal Identification Number (PIN). External (non-DLA) users may access the system through the use of a CAC or through a logon/password. External user sessions will be automatically dropped after a preset period of inactivity. Internal and external user information is maintained on separate directory servers.

Physical: AMPS servers are kept in a secure, limited access, or monitored work areas accessible only to authorized personnel. PII data is encrypted. Data is backed up daily for reconstruction of the records should the system fail. Access to the servers is Public Key Infrastructure (PKI) controlled. Data is backed up daily.

Technical: AMPS is accredited as part of the Department of Defense Information Technology Certification and Accreditation Process (DITSCAP). It is accessed by DLA users through the use of a CAC and by external (non-DLA) users through the use of a CAC or through a logon/password. DLA computer screens automatically lock upon removal of CAC or after a preset period of inactivity with reentry controlled by reentering the CAC PIN. External user sessions will be automatically dropped after a preset period of inactivity. Managed firewalls prevent access by other systems or network traffic not specifically identified in the firewall rule base. Users can only edit their assigned profile information within their assigned role. Internal and external user information is maintained on separate directory servers. Activity on the system is recorded in an audit log. Audit records cannot be modified or deleted.

19. **Privacy Act Interface:** S500.55, entitled "Information Technology Access and Control Records."

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:**
Threats: Risk of SSN being used for other than "For Official Use Only" has been minimized thru encryption and only displaying to the security officer(s) assigned to manage the specific request. The security officer role/access is only granted to individuals that hold a security officer position. As DLA employees, they are made aware of restrictions on secondary uses of the data records by initial and refresher IA training.

Dangers: There are no dangers in collection and storing in a networked and controlled server. Data stored is accessed only by an authorized individual (security officer).

Risks: Security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

21. **Classification and Publication of Privacy Impact Assessment:**

Classification: Unclassified.

Publication: This document will be published either in full or in summary form on the DLA public Web site, http://www.dla.mil/public_info/efoia/privacy.asp.

DATA OWNER:

Name: [REDACTED] (Signature) 1 Aug 2008 (Date)
Title: Director, J6R Information Operations
Work Telephone Number: [REDACTED]
Email: [REDACTED]

INFORMATION ASSURANCE OFFICIAL:

Name: [REDACTED] (Signature) 4 Aug 2008 (Date)
Title: Information Assurance Manager
Work Telephone Number: [REDACTED]
Email: [REDACTED]

CHIEF PRIVACY OFFICER:

Name: Lewis Oleinick (Signature) 14 Aug 2008 (Date)
Title: Chief Privacy and FOIA Officer
Work Telephone Number: [REDACTED]
Email: [REDACTED]

REVIEWING OFFICIAL:

Name: Mae De Vincentis (Signature) 21 Aug 08 (Date)
Title: DLA Chief Information Officer
Work Telephone Number: [REDACTED]
Email: [REDACTED]